FortiGate Connector for the HPE VAN SDN - Administration Guide

Version 1.0.

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, December 10, 2015

FortiConnector for HPE VAN SDN Controller- Administration Guide

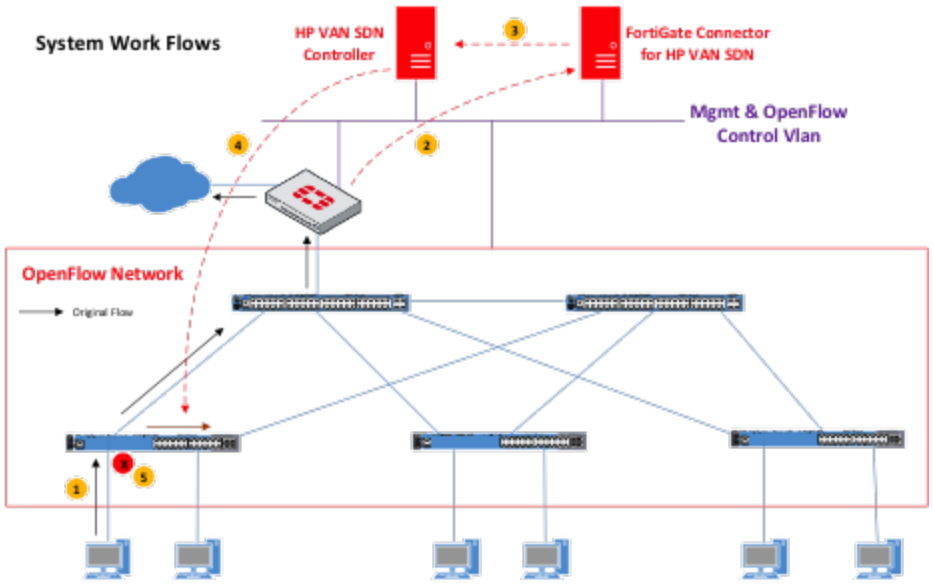
TABLE OF CONTENTS

Change Log

Date	Change Description
2015-12-10	Initial Release

Overview

FortiGate Connector for HP Van SDN version 1.0 is the Fortinet solution that provides the necessary preventative action to isolate an endpoint from the rest of the network in case it generates malicious traffic such that from an exploit or from botnet command and control. The purpose of this preventative action is to block the user's traffic as close as possible to the connected switch and therefore prevent the spread of attack to the rest of the network.



Licensing

FortiGate Connector for HP VAN SDN is free of charge for Fortinet customers. Your FortiGate must be registered with FortiCare at https://support.fortinet.com. Also, you will need to agree with the general Fortinet license agreement. The agreement can be found at http://www.fortinet.com/doc/legal/EULA.pdf.

Features

The FortiGate Connector for HP Van SDN version 1.0 supports the following functions:

- Preventative action based on the results of scans by the AntiVirus engine
- Preventative action based on the results of scans by the Intrusion Prevention System (IPS) engine

- Preventative action based on scans set by parameters in the Application Control Profile
- Preventative action based on scans set by parameters in the Web Filter Security Profile

Supported Products

FortiGate products

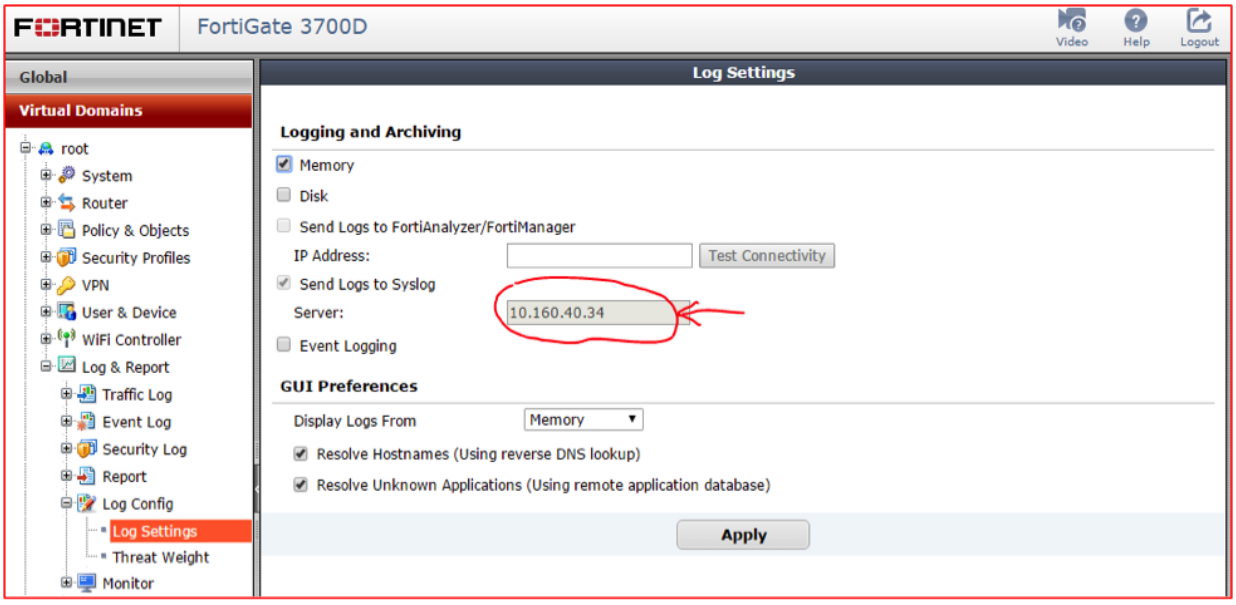
- All physical FortiGate devices running:
  - FortiOS 5.2
  - FortiOS 5.4
- A versions of FortiGate-VM running:
  - FortiOS 5.2
  - FortiOS 5.4

HP products

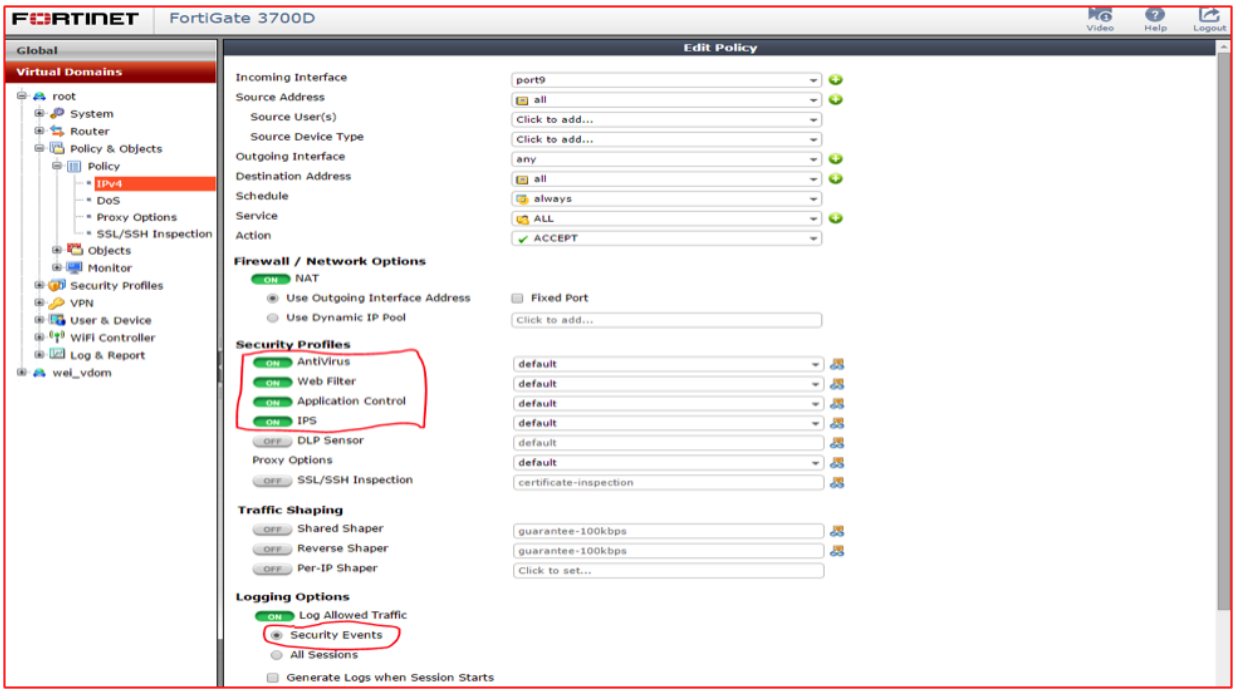
- HP VAN SDN Controller version: 2.5.15
- HP Switch version: KA.15.18.0006

Prerequisites

• The FortiGate Connector IP address should be entered in the field for the Syslog server IP address on the FortiGate.



• In order for the FortiGate Connector to make use of the ***Security Profiles***, the profiles, as well as the ***Security Events*** option, need to be enabled on the FortiGate.


FORTINET
FortiGate 3700D
Video
Help
Logout
Global
Virtual Domains
root
System
Router
Policy & Objects
Policy
IPv4
DoS
Proxy Options
SSL/SSH Inspection
Objects
Monitor
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
wei_vdom
Edit Policy
Incoming Interface
port9
Source Address
all
Source User(s)
Click to add...
Source Device Type
Click to add...
Outgoing Interface
any
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Firewall / Network Options
NAT
Use Outgoing Interface Address
Fixed Port
Use Dynamic IP Pool
Click to add...
Security Profiles
AntiVirus
default
Web Filter
default
Application Control
default
IPS
default
DLP Sensor
default
Proxy Options
default
SSL/SSH Inspection
certificate-inspection
Traffic Shaping
Shared Shaper
guarantee-100kbps
Reverse Shaper
guarantee-100kbps
Per-IP Shaper
Click to set...
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Generate Logs when Session Starts

Installation

FortiGate Connector for HP VAN SDN is packaged in a VmWare OVF file. In order to deploy FortiConnector for HPE VAN SDN Controller the file `FortiConnector_v1.0.ovf` on VMware EXSi 5.5 needs to be used.

Change Default root password

The default root credentials for FortiGate Connector for HP VAN SDN are:

- User name = `forticonnector`
- Password = `fortinet`

The user name cannot be changed but the password can be changed using the following steps:

1. Use the default root credentials to login to the FortiGate Connector.
2. At the prompt execute the following command:
   `passwd`
   The results will be:
   ```
   Changing password for forticonnector.
   (current) UNIX password:
   ```
3. Enter the current password which should be the default password `fortinet`.
   `Enter new UNIX password:`
4. Enter the new password that you want to use.
   `Retype new UNIX password:`
5. Verify the password by retyping it.If all done correctly the result should be:
   `passwd: password updated successfully`

Change default IP address

The default IP address is 192.168.99.1.

The IP address can be changed using the following command:

```
sudo ifconfig eth0 <new_IP_address> netmask <new_subnet_mask>
```

Change default GUI management credential

The default login credentials of the GUI management interface are:

- User name = `admin`
- Password = `admin`

The user name and password can be changed using the following steps:

1. Use root credential to login FortiGate Connector console
2. Use the `cd` command to go to the directory with the config folder
   `cd /home/forticonnector/workspace/sdn_hp/config`
3. Use vi to open the password file using the folllowing command:
   `vi fsdn_passwd.text`
4. Use vi to modify user name and password.

Set system clock

The system clock needs to be set accurately to make sure it is in sync with the clock in the HP VAN SDN controller.

To configure time zone:

```
sudo dpkg-reconfigre tzdata
sudo /etc/init.d/cron stop
sudo /etc/init.dcron start
```

To configure clock:

Use the following command to manually set a specific date and time:

```
sudo date –set=”2015-12-09 13:52:52”
```

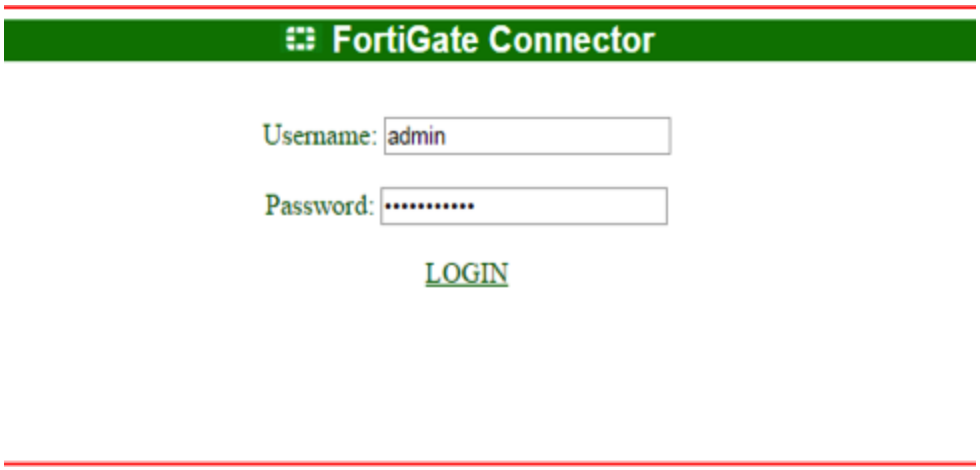
Option:

You can use the standard Ubuntu method to install the NTP daemon and enable NTP to sync the system clock with a time server on the Internet. The advantage with this method is that once set up, you don't have to worry if your clock speed is slower or faster than the controller's. You can install the daemon with:

```
sudo apt-get install ntp
```

Login Page

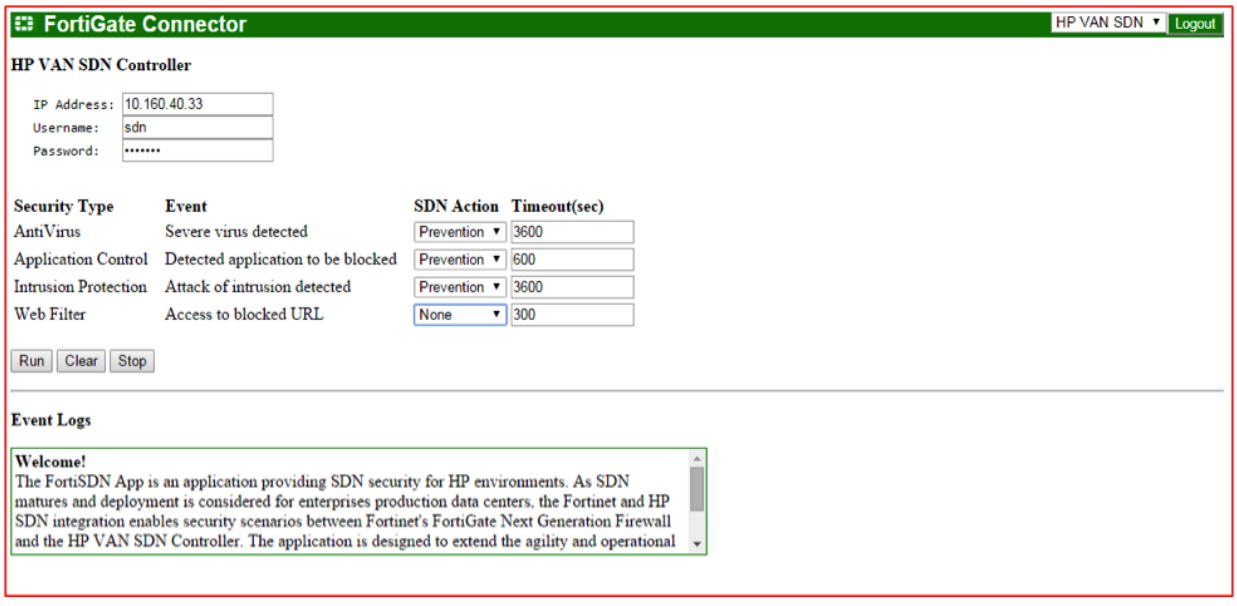
Loging into the GUI management interface is done by using the HTTPS prefix and the device's address in your browser as a URL. The default URL would be `https://192.168.1.99`. If the default IP address is still in use but your computer's address on a different subnet you will need to temporarilty change the IP address of your computer to be on the same subnet.



Configuration Page

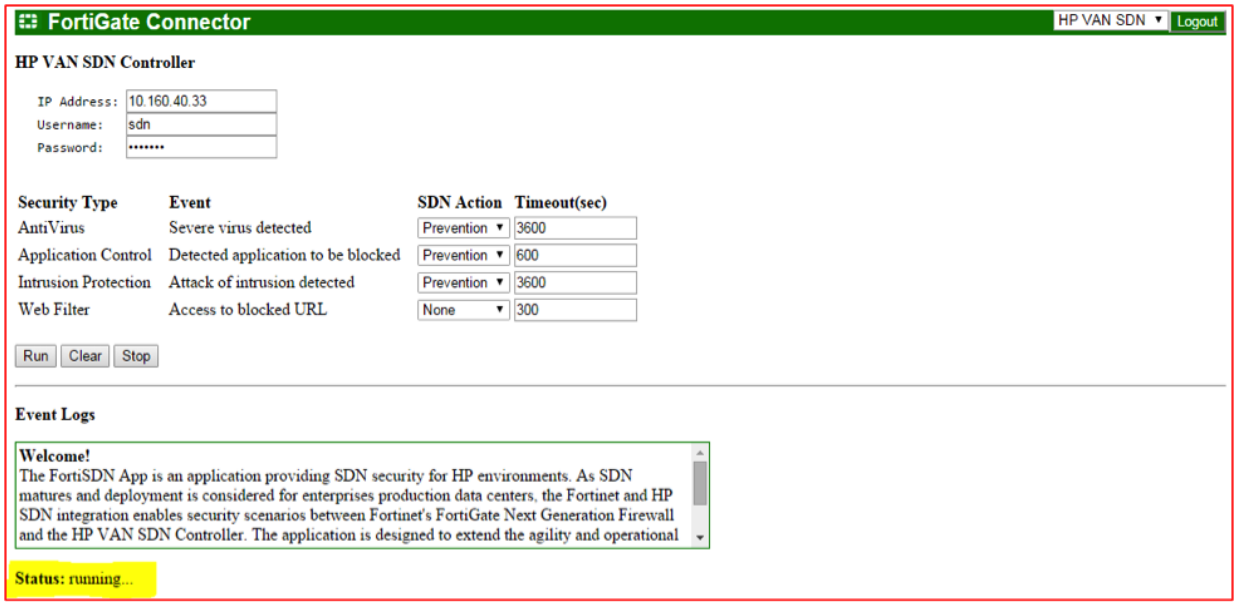
Once on the configureation page of the the FortiGate Connector there are some configuration settings that may need to be changed to integrate the device and set the preferences for your network:

- Configure the IP address for the HP VAN SDN Controller
- Configure the access credentials for the HP VAN SDN Controller
- Configure Action type for each secuity type
- Configure flow Timeout value for each security type.(Enter 0 for default timeout value 600 seconds)



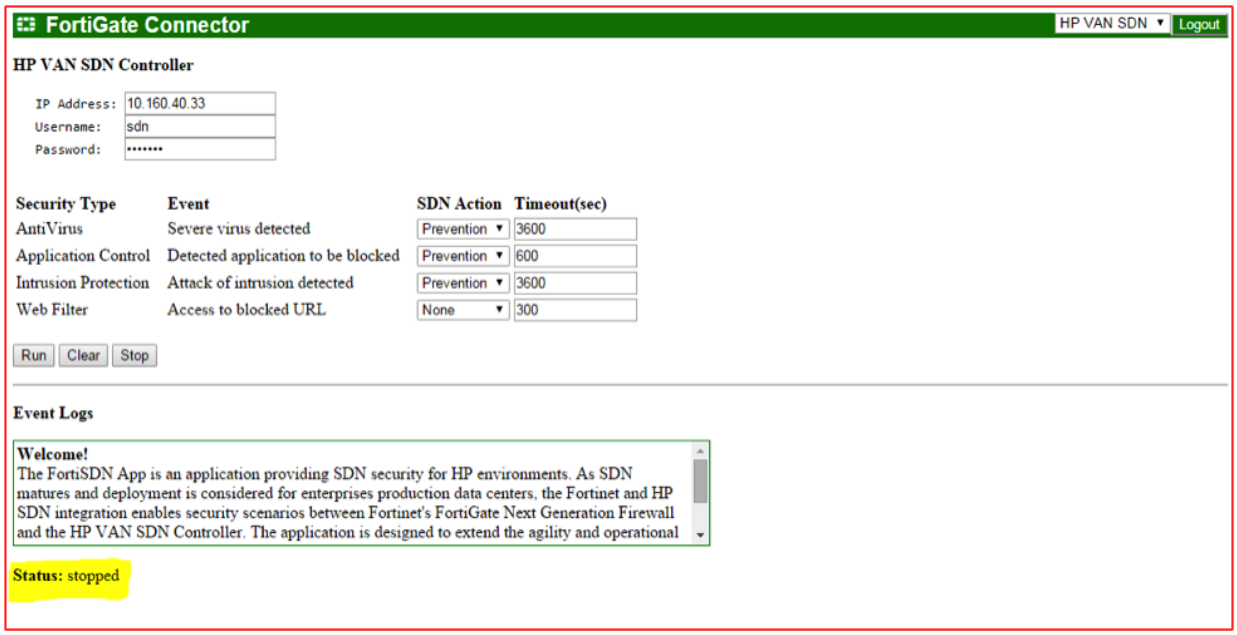
Starting the FortiGate Connector

Once the correct settings have been configured select the ***Run*** button.The application should start. When the ***Status*** indictor displays "***running ...***", it means the FortiGate Connector is ready to receive Syslog information from the FortiGate and to push the flows to the HP VAN SDN Controller.



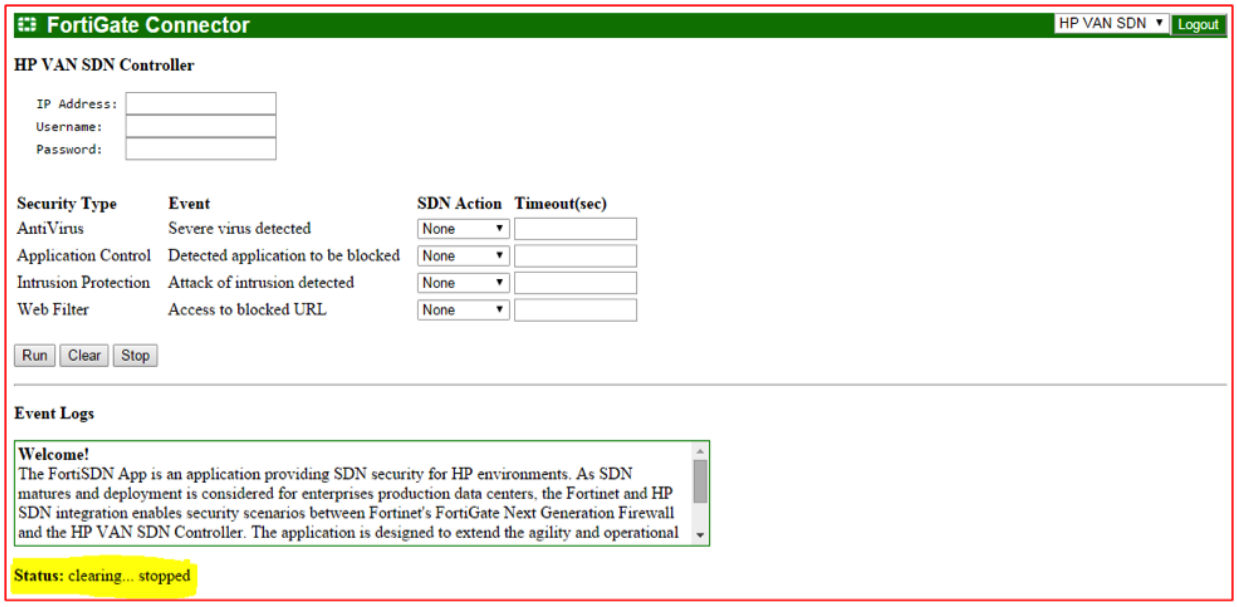
Stopping the FortiGate Connector

To stop the FortiGate Connector, select the ***Stop*** button. The ***Status*** indicator will display "***stopped***".This means FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, but the all the configurations are unchanged and maintained.



Clear the configuration and stop FortiGate Connector

To clear the FortiGate Controller, select the ***Clear*** button.The application will stop and configurations will be cleared. When the ***Status*** indicator displays "***clearing…stopped***", it means the FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, and has cleared previous configurations.



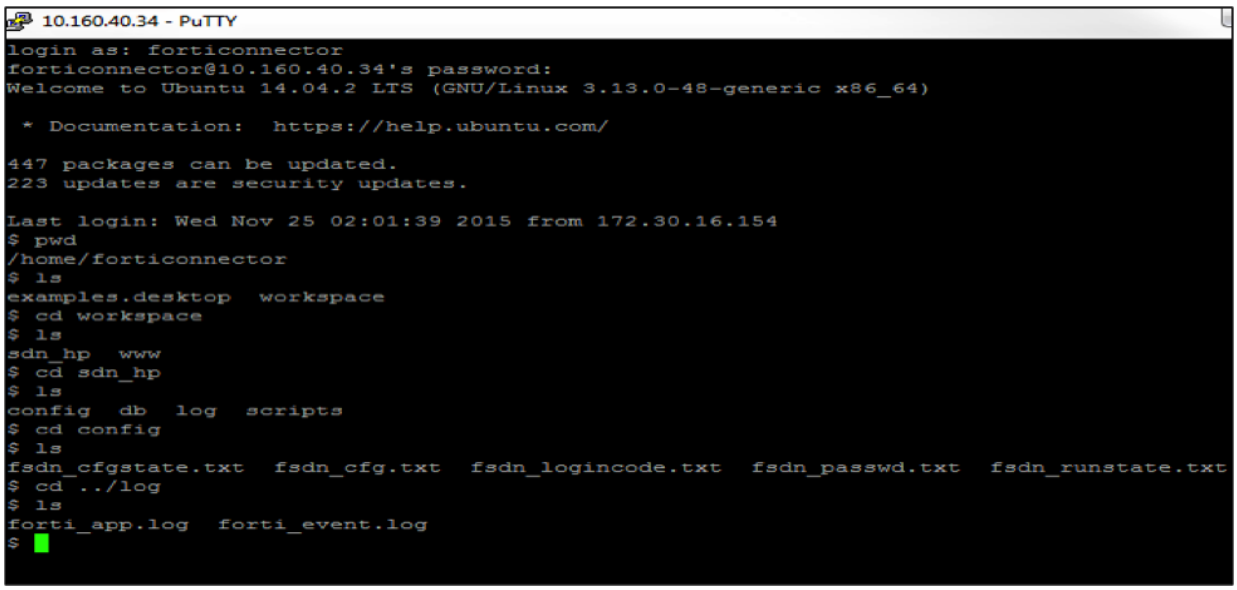
Supported use scenarios

- When a user sends a malware file through the network and the FortiGate detects it, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the listening port number, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all matching application traffic from this user's IP address. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all traffic from the user's IP address to the website's IP address. Traffic from the user to other websites is not affected.

Basic Troubleshooting

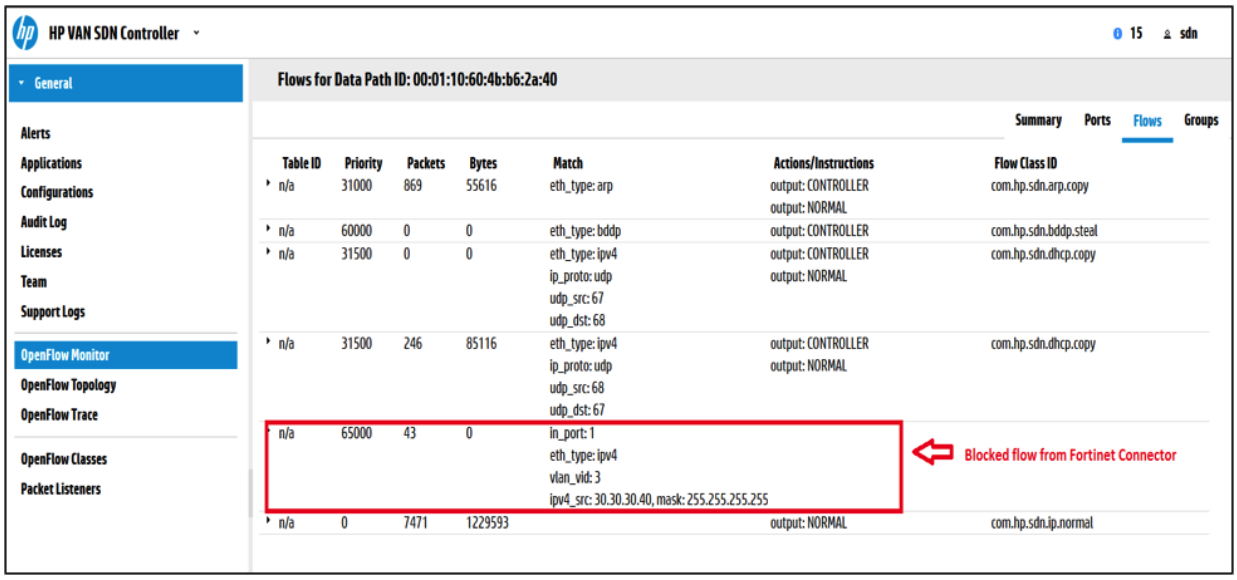
The following are some quick pieces of information that may be helpful in troubleshooting issues that may come up while administering your FortiGate Connector:

- The configuration file is located in the folder: `/home/forticonnector/workspace/sdn_hp/config/`
  - The file is: `fsdn_cfg.txt`.
- Debug messages and event logs are located in the following files:
  - `forti_app.log`
  - `forti_envent.log` (contains events only)
- The syslog messages from the FortiGate are located in the folder: `/var/log/syslog`.



Verify flow pushed by FortiGate Connector on HP SDN Controller

In order to verify flows pushed by the FortiGate to the HPE VAN SDN Controller, navigate to the flow page on the HPE VAN SDN Controller.

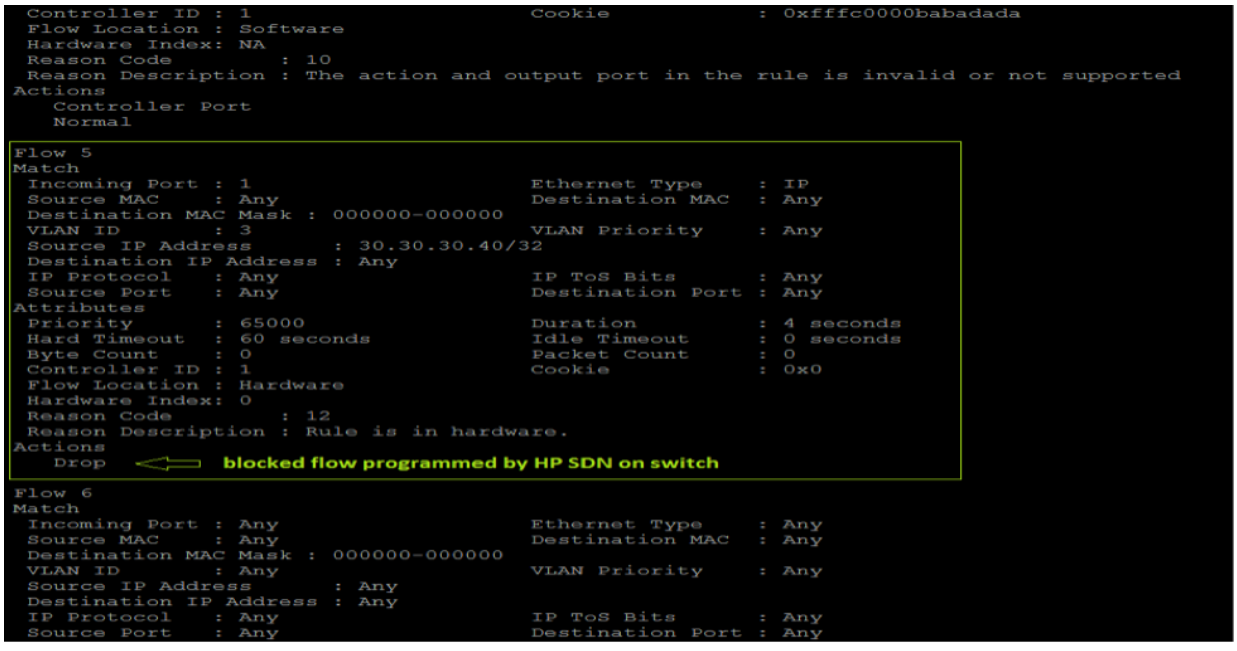


Verify flow pushed by FortiGate Connector on HP switch

In order to verify flows pushed by the FortiGate to the HPSwitch

1. Login to the HP switch console.
2. Issue the following command:

```
HP-Switch# show openflow instance aggregate flows
```



FORTINET

High Performance Network Security